Shared-Resource Management Using Online Social-Relationship Metric for Altruistic Device Sharing

Inagaki, Yuichi; Shinkuma, Ryoichi

SPECIAL SECTION ON SOCIAL COMPUTING APPLICATIONS FOR SMART CITIES

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 25, 2018, accepted March 30, 2018, date of publication April 6, 2018, date of current version May 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2823300

Shared-Resource Management Using Online Social-Relationship Metric for Altruistic Device Sharing

YUICHI INAGAKI AND RYOICHI SHINKUMA
Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan
Corresponding author: Yuichi Inagaki (yinagaki@icn.cce.i.kyoto-u.ac.jp)

This work was supported by the Research Grant from the KDDI Foundation, Japan.

ABSTRACT The confluence of two emerging paradigms, Internet of Things and sharing economy, has encouraged people to share their assets, which could include personal devices, with others. A typical example of such altruistic device sharing is ''tethering'' in cellular networks: an owner who uses a smartphone relays data from/to base stations for others who do not have direct connectivity to cellular networks. However, when people share devices, they would be concerned about costs such as battery or bandwidth. Device owners generally want to reduce their costs when they share their devices with someone who is less socially close to them. This is because it was reported that our altruistic behavior has clear correlation with social closeness; the less close someone is to you, the less altruistic actions you take towards that person. Therefore, we propose a system that uses online social relationships to meet device owners' demand for shared-resource management to enable altruistic device sharing. By acquiring and evaluating online social relationships between a device owner and user, the proposed system automatically determines how much resources the user is allowed to use. In this paper, we implemented a prototype system to measure its authentication overhead. Using this actual overhead measured on the prototype system, we conducted a simulation with a large-scale data set of a real social network to verify that: 1) the proposed system limits the resource usage for guest users who are not as close to the device owners and 2) the overhead of the authentication process in the proposed system does not interfere with the resource sharing with guest users who are close to the device owners.

INDEX TERMS Social closeness, device sharing, resource management, sharing economy.

I. INTRODUCTION

Over the past several years, we have witnessed great progress in wireless communications and digital electronics. These advances have enabled an increasing number of devices, such as tablets, sensors, wearable devices, robots, and autonomous cars, to be connected to the Internet. Due to the spread of the Internet-of-Things (IoT) paradigm, even everyday items, such as food packaging, furniture, and paper documents, will be Internet nodes by 2025 [1]. In addition to this change, a global trend toward peer-to-peer sharing of personal assets has been suggested. This trend is called the ''sharing economy'' and is demonstrated in services such as Airbnb, Uber, and Freecycle. The sharing economy was nominated by Time in 2011 as one of ''10 ideas that will change the world'' [2]. Furthermore, the global annual revenue of the sharing economy, which was $15 billion in 2015, has been estimated to grow to $335 billion by 2025 [3].

Due to the confluence of the above two paradigms, i.e., IoT and sharing economy, various devices owned by a person will be shared with others. For example, members of a global WiFi sharing community called FON [4] share their WiFi routers with other members. Another example is mobile cloud [5], [6]. By sharing computing resources with mobile devices, mobile cloud attains more powerful computing than stand-alone computing and enables mobile devices to offload computing tasks with low levels of latency. Sensing devices in wireless sensor networks (WSNs) are also shared for various purposes. SenseWeb is an infrastructure for shared sensing, which provides greater understanding by collecting sensing data from multiple different networks [7]. Sharing airborne sensors enables efficient use of their spare sensing resources [8], [9]. A system called eShare enables energy exchange among shared sensors [10].

When a device owner decides how much or how long her or his device can be shared with others, it is a good idea to consider how close these others are to the device owner. There are two reasons for this. First, social closeness has a strong relationship with our daily mobility patterns. We have more chance to encounter someone if she or he is socially close to us. Eagle and Pentland [11] introduced a system to collect data from mobile phones and studied the relation between the logged data and social nature of the subjects. They revealed that social closeness between people is strongly correlated with their contact logs. Hui *et al.* [12] proposed a delay-tolerant network (DTN) based on social metrics. To infer human communities and select forwarding paths, they measured the social closeness between two people by the number of contacts and how long they spend together. Second, the social closeness between people has a correlation with how altruistic someone will be to others [13]–[17]. For example, when devices are shared among people, the owners do not want to share their devices with strangers, while they are more willing to share their devices with their socially closer friends or families. The less socially close the guest user is to the device owner, the less altruistic the device owner becomes.

Device-sharing systems need to meet demands in which device owners want to restrict less socially close users from using the resources of the owners' devices. A typical example of altruistic device sharing, which we will focus on in Section IV, is 'tethering' in cellular networks: an owner who uses a personal device such as a smartphone, which has direct connectivity to cellular networks such as 3G, long-term evolution (LTE), or LTE-Advanced (LTE-A), relays data from/to base stations (BSs) for others who do not have direct connectivity to cellular networks but connect their PCs or tablets to the owner's device via WiFi [18]. Tethering incurs costs such as those imposed by battery life or bandwidth [19]. When device owners offer tethering, they want to save the costs to guest users who are not as close to them because they are less altruistic to such users. However, to the best of our knowledge, conventional device-sharing services do not meet such demand. They do not allow device owners to vary the authorized level of resource usage of guest users or only allow device owners to manually manage the authorized level of resource usage of users, which imposes a great burden on device owners.

Therefore, we propose a system that uses online social relationships to meet device owners' demands for resource management to enable altruistic device sharing. When a shared device receives a connection request from a guest user, the shared device first sends a request to the authentication server. Then, the authentication server evaluates online social relationships and determines how much of a resource on the shared device can be used by a guest user. We also present a prototype implementation and a large-scale simulation using a dataset of a real social network to verify that i) the proposed system limits the resource usage for guest users who are not as close to the device owners, and ii) the overhead of the authentication process in the system does not interfere with the resource sharing with guest users who are close to the device owners.

Several studies have been carried out that are similar to ours. Shankar *et al.* proposed and demonstrated an architecture called SBone, which allows personal devices to seamlessly and securely share their resources and state with each other by using a social network for authentication, naming, discovery, and access control [20]. They suggested that SBone would be applicable to situations in which a device owner provided her or his Internet connectivity to others who were friends with her or him in online social networks. Another similar effort has been in communication with social-aware device-to-device, which directly share data between mobile devices used by people who have social relationships without using infrastructure networks such as cellular networks [21]–[23]. However, these prior studies did not consider how shared resources were to be managed on the basis of social closeness between owners and users.

The rest of this paper is organized as follows. Section II introduces prior efforts related to device sharing and applications that use online social relationships. Section III presents the architecture and resource management procedures for the proposed system. Section IV provides a prototype implementation and simulation results that validate the performance and effectiveness of the proposed system. Finally, Section V concludes the paper.

II. RELATED WORK

A. TECHNOLOGIES FOR DEVICE SHARING

This section presents prior efforts related to device sharing in a society in which devices are shared actively. In most of these device-sharing services, the authorized level of resource usage can be controlled. However, it is difficult to determine the appropriate authorized level of resource usage for each user according to device owners' demand.

FON is one of the most widely used communities of global WiFi sharing [4], [24]. FON provides a platform for members of the community to share their spare bandwidth with other members. Those who join the FON membership are known as Foneros. A Fonero buys a local FON wireless router and shares their spare bandwidth with other Foneros. In return, a Fonero has free access to the FON's WiFi network, which consists of over 20 million hotspots worldwide, and enjoys wireless Internet connection.

A cloudlet is a small-scale cloud datacenter that is located on the edge of the Internet and offers resources for mobile cloud computing [5]. Mobile devices have only limited computational resources, such as power, memory, storage, and energy, compared to static devices. To help these resource-poor mobile devices save computational resources, a cloudlet server is connected to the mobile devices through various short-range radio communication technologies. A cloudlet offers mobile cloud computing, which offloads computational tasks of mobile devices with low latency. Nishio *et al.*

proposed a service-oriented mobile cloud for sharing heterogeneous resources such as CPUs, bandwidth, and content [6]. They suggested that service-oriented heterogeneous resource sharing achieves low latency and high energy efficiency in a mobile cloud environment.

Sensor sharing in WSNs is also a common example of device sharing. Microsoft developed an infrastructure for shared sensing called SenseWeb. By sharing sensors that were originally used for a specific application and placing those sensors into a single development system, SenseWeb enables production of new types of media and sensing applications over existing data networks [7]. Airborne sensors are also shared. Since airborne sensors are typically idle for much of their flight time, efficient sensing can be achieved by sharing airborne sensors and allowing other information consumers to opportunistically use them during their otherwise idle time [8], [9]. Sensors are also shared to exchange energy. A system called eShare enables networked sensor systems to robustly extend their lifetime by exchanging energy with shared sensors [10].

Some systems that share peripheral input/output (IO) devices through a network have been proposed. A peripheral bus extension called universal serial bus/internet protocol uses a virtual peripheral bus driver that enables users to share various devices over an IP network [25]. A USB cross-platform extension has also been developed to share peripherals in a heterogeneous environment via a transmission control protocol/internet protocol network [26]. A system called CameraCast provides a logical device application programming interface (API) that enables an application to gain system-level access to a remote video-sensor device [27]. Composable IO is a resource-sharing technology that enables IO peripherals to be shared among cloud computing members [28].

B. APPLICATIONS USING ONLINE SOCIAL RELATIONSHIPS

This section discusses prior work related to applications that use online social relationships. Various metrics can be extracted from online social relationships; therefore, there has been extensive research on exploiting online social relationships to control networks. However, to the best of our knowledge, our work is the first on resource management for device sharing that enables device owners to control the authorized level of shared-resource usage according to their online social-relationships with device users.

An example of routing in a delay-tolerant mobile ad hoc network (MANET) involves performing community detection based on a dynamic online social relationship with frequent changes introduced by users joining or withdrawing from one or more groups or communities by friends connecting with each other or by new people making friends with each other [29]. Wang *et al*. proposed a framework of traffic offloading assisted by social networking services (SNSs) via opportunistic sharing in mobile social networks. Their framework pushes the content object to a properly selected group of seed users, who will opportunistically meet and share the content with others, depending on their spreading impact on the SNS and their mobility impact [21]–[23]. Through extensive trace-driven simulations, they demonstrated that their framework can drastically reduce mobile traffic load in cellular networks, while all users' access delay requirements can be satisfied.

Kyle *et al*. suggested that online relationships in social networks are often based on real-world relationships and can therefore be used to infer a level of trust between users. On this hypothesis, they proposed to leverage those online relationships to form a dynamic "Social Cloud"; thereby, enabling users to share heterogeneous resources [30], [31]. They actually implemented a social storage cloud application using the Facebook API, in which online storage is shared by people having online relationships on Facebook.

Not only relationships between people but also relationships between content and people can be taken into consideration when distributing content in a network [32]. Based on metrics produced from relationships between people and content, routers and content on the network can be managed physically to achieve load balancing, low-retrieval latency, and privacy while distributing content. Community detections from online social relationships can be used for creating a community-associated virtual network [33]. Physical network resources are assigned to each community-associated network using a network virtualization technique. In a community-associated network, people can exchange privacy-sensitive data with only a small risk of data being disclosed to people who they are not socially connected to.

C. METRICS FOR ANALYZING SOCIAL RELATIONSHIPS

This section presents several common metrics that help us analyze social relationships between users.

Communities on most SNSs can be explicitly created by users. For example, such communities are called "groups" on Facebook. However, communities can be detected from the network topology by using community-detection algorithms. Link communities [34] detect communities that users belong to by hierarchically clustering the links between users. The most remarkable feature of this algorithm is that it allows users to belong to multiple communities.

In addition to communities, one-to-one relationships between two users can also be used to analyze social relationships. The one-to-one relationship between users x and y can be represented by $E(x, y)$. The $E(x, y)$ in common neighbors [35] is given as

$$E(x, y) = |\Gamma(x) \cap \Gamma(y)|, \tag{1}$$

where $\Gamma(z)$ is the set of neighbors of a node z. It is assumed that two users who share many common neighbors are likely to have a stronger relationship. The $E(x, y)$ in the Jaccard Index [36] is given as

$$E(x, y) = \frac{|\Gamma(x) \cap \Gamma(y)|}{|\Gamma(x) \cup \Gamma(y)|}. \tag{2}$$

It is assumed that two users have a stronger relationship when the set of their common neighbors matches well. The $E(x, y)$ in the Adamic-Adar Index [37] is given as

$$E(x, y) = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{\log k_z}, \tag{3}$$

where k_z is the degree of a node z. It formalizes the intuitive notion that rare features are more important. The $E(x, y)$ in the Katz Index [38] is given

$$E(x, y) = \sum_{l=1}^{\infty} \beta^l \cdot |\text{paths}_{xy}^{\langle l \rangle}| \tag{4}$$

$$= \beta A_{xy} + \beta^2 (A^2)_{xy} + \beta^3 (A^3)_{xy} + \cdots, \tag{5}$$

where $\text{paths}_{xy}^{\langle l \rangle}$ is the set of all paths with length l connecting x and y, β is a free parameter controlling the path weights, and A is the adjacency matrix: $A_{xy} = 1$ if x and y are directly connected and $A_{xy} = 0$ otherwise. Note that, $(A^l)_{xy}$ is equal to the number of paths of length l from x to y. It gives the shorter paths greater weight.

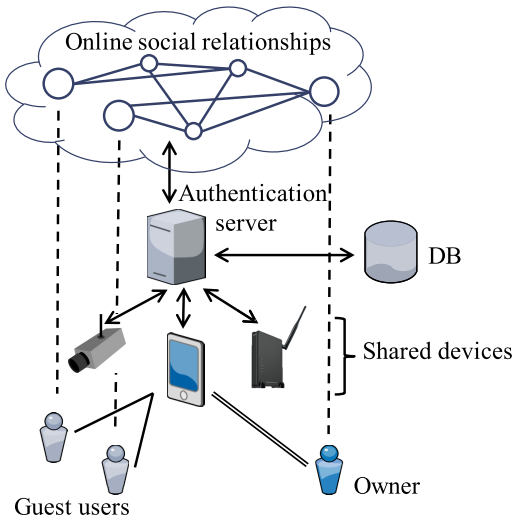

FIGURE 1. Proposed system architecture.

III. PROPOSED SYSTEM DESIGN

A. SYSTEM ARCHITECTURE

The proposed system architecture (Fig. 1) consists of four components: (a) an authentication server, (b) shared devices, (c) owners, and (d) guest users. The authentication server manages the shared devices and the online social account information of the owners and guest users. The authentication server determines which guest user can access which function or resource of the shared devices according to the relationship between the owners and guest users. A centralized architecture is adopted for the authentication server, so it can easily manage online social relationships between the owners and guest users. The shared devices are devices that can be accessed by guest users, such as tablets, sensors, wearable devices, robots, and autonomous cars. Each shared device belongs to one owner. The guest users are granted access to the shared devices according to the online social relationship with the owner of the shared devices.

B. OWNER-RELATED PROCEDURES

1) DEVICE REGISTRATION

An owner registers her or his personal devices on the authentication server before the owner starts to share the devices. When an owner registers a device, the authentication server issues a unique ID to the device. The authentication server associates the device ID with the owner's online social account information and records them in a database (DB).

2) SOCIAL-CLOSENESS EVALUATION FROM EXTRACTED SOCIAL RELATIONSHIPS

The proposed system requires i) a data source from which the proposed system obtains online social relationships and ii) a metric by which the proposed system quantitatively analyzes the online social relationships to use those relationships between owners and guest users to manage resources.

One of the most common and familiar examples of online social relationships is found in online social networks (OSNs) [39]. OSNs are offered by SNSs such as Facebook, Twitter, Google+, and LinkedIn. OSNs consist of nodes and edges. Nodes represent users (more specifically, online social accounts of users) of OSNs, while edges represent social interactions among these users. Note, in this section, users mean not device users but SNS users. The most basic social interactions that are represented by edges are friendships. Although some OSNs adopt undirected friendships and others adopt directed friendships, both types of friendships are included in online social relationships. Comments, messages, and reactions to other users are also examples of online social relationships, apart from friendships.

Several common metrics can be used to analyze the social closeness between users, as described in Section II-C. By using communities and one-to-one relationships between two users, the proposed system defines the social closeness between x and y as

$$SC(x, y) = \begin{cases} 0 & \text{if } x \text{ and } y \text{ are not friends, or} \\ & \text{they do not belong to the same} \\ & \text{community} \\ E(x, y) & \text{otherwise,} \end{cases} \tag{6}$$

where $E(x, y)$ is an index that represents the one-to-one relationships between x and y, as defined in Section II-C.

C. USER-RELATED PROCEDURES

The authentication flow of the proposed system is illustrated in Fig. 2. Details of each message in Fig. 2 are described in Table 1. Authentication consists of two phases: identification and authorization. The authentication server identifies guest users in the identification phase (1.1–1.4) by using their online social accounts. The authentication server

TABLE 1. Details of exchanged messages.

Message name	Content data name	Details
(1.1) share_request	guest_id	ID to identify guest user
(1.2) redirect	authentication_url	Uniform resource locator (URL) of authentication server's endpoint
(1.3) identification_request	guest_id	See above
	shared_device_id	ID to identify shared device
	social_account_id	ID of a social account of guest user
	social_account_pass	password of social account of guest user
(1.4) identification_response	access_token	Secret key to access online social relationships
(2.1) authorization_request	access_token	See above
	owner_id	ID to identify owner
	guest_id	See above
(2.3) authentication_response	resource_management_info	Information to control access from guest users e.g., authorized connection time
(2.4) share_response	resource_management_info	See above

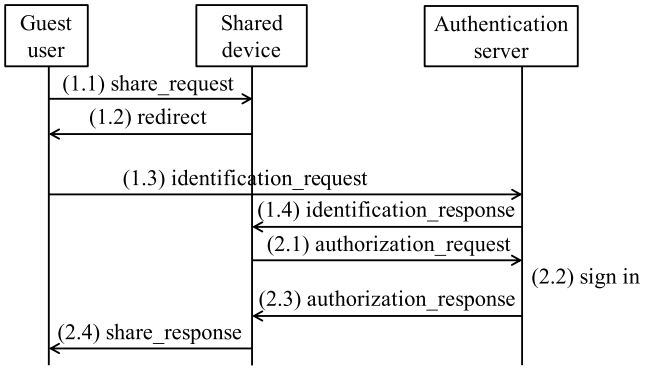

FIGURE 2. Authentication flow.

acquires the online social relationships between the owner and guest user, then the shared devices control the access for the guest user based on the relationships in the authorization phase (2.1–2.4).

1) IDENTIFICATION

(1.1) A guest user requests access to the shared device. (1.2) The shared device requests the guest user to sign in to the authentication server. (1.3) The guest user signs in to the authentication server with the guest user's online social account. (1.4) The authentication server notifies the shared device that the guest user has completed signing in to the authentication server.

2) AUTHORIZATION

(2.1) The shared device requests the authentication server to authorize the guest user. (2.2) The authentication server acquires online social relationships between the owner and guest user. The authentication server creates access control information based on these relationships that define whether the guest user can access the shared device and the authorized level of resource usage for the guest user. (2.3) The authentication server issues the resource-management information to the shared device. (2.4) The shared device controls access for the guest user based on the received information.

D. ADVANTAGES AND DISADVANTAGES

With the proper use of online social relationships, we can develop services that meet the demand of smart cities. By combining information acquired from social relationships with free WiFi and business support, the proposed system can be extended to a smart city product. For example, Bumbee Labs in Sweden has offered free WiFi to tourists to acquire their mobility logs and analyze them to increase B to B sales [40]. Combining online social relationships with those data will help such services offer more valuable and interesting analysis.

However, we should also note that online social relationships may lead to privacy issues. A major concern is that one user may be able to infer some private information of another user. As future work, we will investigate how the social relationships are prone to raise such a risk.

IV. PERFORMANCE EVALUATION

In our performance evaluation, we assumed a tethering scenario, in which a device owner relays data to cellular networks, such as LTE, for other guest users who connect their PCs or tablets to the owner's mobile device, such as a smartphone, via WiFi [18]. Section IV-A introduces an implementation of a prototype system and the performance measurement of the prototype system to confirm that the authentication overhead is within a realistic range. Using the authentication overhead actually measured (Section IV-B) presents a simulation with large scale and real social network data to verify i) and ii) mentioned in Section I.

For the rest of this section, authorized connection time is used as an index of the authorized level of resource usage. The authorized connection time is the duration in which guest users are permitted to connect to shared devices.

A. PROTOTYPE IMPLEMENTATION

1) OVERVIEW

The architecture of the implemented prototype system is illustrated in Fig. 3. This prototype system selects the WiFi access point (AP) as a shared device and uses the number of common neighbors on Facebook as an indicator of social

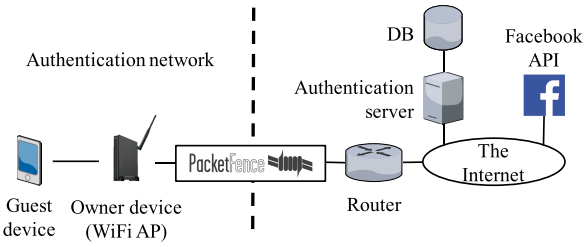

FIGURE 3. Implemented prototype system.

closeness. The number of common neighbors [35] is used as a metric, as described in Section III-B to control the authorized connection time for guest users to access the Internet through the AP. To delegate guest-user identification management to Facebook accounts, the OAuth protocol is used. In addition, the implemented prototype system adopts a system called PacketFence to control the packet flow through the AP. PacketFence communicates with the authentication server and guest device and performs access control on behalf of the shared WiFi AP.

The authentication flow is composed of the identification and authorization phases. In the identification phase, the guest user requests access to the shared device and signs in to the authentication server with the guest user's Facebook account. The authentication server identifies the guest user by receiving the guest user's information from Facebook. The authentication server and PacketFence communicate with each other to exchange the guest user's pieces of information such as the guest user's name or email address. In the authorization phase, the authentication server obtains the number of common friends between the owner and guest user and determines the authorized connection time for the guest user to access the WiFi AP.

Under this configuration, the implemented prototype system allows the guest users to connect to the Internet through the AP without entering complex WiFi passwords as long as they have a Facebook account.

2) DETAILS

a: FACEBOOK API

Facebook offers one of the largest OSNs in the world [41] and offers rich APIs. Facebook APIs allow the implemented prototype system to use various data on Facebook easily. The number of common neighbors is an example of various data offered by Facebook through the APIs. These indicators represent the social closeness among users well; therefore, they are suitable for controlling the authorized connection time for each user.

b: OAuth

OAuth is a protocol that enables a third-party application to access resources on a hypertext transfer protocol (HTTP) service on behalf of a resource owner [42]. The OAuth protocol flow consists of the following three main parts. (1) The resource owner is identified by the HTTP service and approves the third-party application's access to the resource. (2) The third-party application receives an access token from the authorization server of the HTTP service. (3) The third-party application requests the protected resource on the resource server of the HTTP service by presenting the access token.

In the implemented prototype system, Facebook, online social relationships on Facebook, and the authentication server of the implemented prototype system represent the HTTP service, resource, and third-party application, respectively. By using the OAuth protocol, the implemented prototype system gains two benefits. First, the implemented prototype system can delegate the identification of users to Facebook. This saves the system the trouble of managing passwords or user accounts on its own. Second, the implemented prototype system can acquire online social relationships from Facebook for access control on behalf of the users.

c: PACKETFENCE

The packet flow through the AP is controlled by a system called PacketFence, which is a free and open source network access control solution [43] that can be deployed under the following three types of enforcement: inline, out-of-band, and hybrid. The implemented prototype system adopts inline enforcement, which is the most basic and simple enforcement among the three. Under inline enforcement, the PacketFence server is placed between a router connected to the Internet and an authentication network that includes the shared AP and guest user devices. Therefore, all packets exchanged between the authentication network and Internet must go through the PacketFence server. When a packet from an authorized guest user device attempts to go through the PacketFence server to outside the authentication network, the PacketFence server behaves like a normal router and allows the packet to pass. On the other hand, when a packet from an unauthorized guest user device attempts to do the same thing, the PacketFence blocks the packet and displays a captive portal that prompts the guest user to sign in.

The flexible design of PacketFence allows the implemented prototype system to add a module to exchange authentication information with the authentication server.

3) PERFORMANCE MEASUREMENT

a: METRIC

This section adopts the time required for authentication as a metric of authentication overhead. However, the time consumed while the user enters her or his username and password on the sign-in page of Facebook should not be included in the measurement because it varies from person to person. Therefore, we assume that the user usually uses Facebook with a browser on the user's device, i.e., the user has already signed in to Facebook and a Facebook credential has been stored in a browser cookie. Under this assumption, the sign-in procedure is completed as soon as the user visits the sign-in page of Facebook, and the time taken to enter the username and password is not included in the measurement.

TABLE 2. Details of experimental setup.

OS	CentOS 6.8
Memory	8 GB
CPU	Core i7-860 2.8 GHz × 8
No. of measurements	25
PacketFence version	6.3.0
Guest device	iPhone 7 iOS 11.2.2
Browser on guest device	Google Chrome
Authentication server	Ruby 2.3.1, Rails 4.2.7, on Heroku

b: EXPERIMENTAL SETUP

The details of the experimental setup are listed in Table 2. PacketFence was installed on a CentOS machine. The authentication server was implemented as a Ruby on Rails web server and deployed on one of the most popular platforms as a service (PaaS) called Heroku.

The time required for authentication was extracted from timestamps in a log file of the authentication server. In this measurement, the time required for authentication is defined as the length of a period that begins with the first request to the server and ends with the last response from the server.

c: REFERENCE SETUP

The reference system does not take into account the online social relationships between a device owner and guest users. The authentication server in the reference system does not acquire and evaluate online social relationships on Facebook and allows all guest users to use the WiFi AP for a fixed duration.

TABLE 3. Time required for authentication.

	5th (s)	median (s)	20th (s)
Reference	4.786	5.086	6.216
Proposed	5.196	5.408	5.800

d: RESULTS

Table 3 shows the duration required for authentication, which was measured using the prototype system. In the table, the 5th shortest, median, and 20th shortest values obtained from 25 measurements are shown for evaluating the distribution of the measured duration. The median of the duration required for authentication in the proposed system was slightly longer than that in the reference system. This is because the proposed system acquires and evaluates online social relationships on Facebook, while the reference system does not. However, this duration was not dominant in the entire authentication process. These results verified that the proposed system works sufficiently in terms of the overhead for authentication compared with the reference system.

B. SIMULATION WITH REAL DATA

1) EVALUATION SCENARIO

In the previous section, we discussed measuring the authentication overhead. In this section, using the measured overhead, we discuss a simulation we conducted to verify i) and ii) mentioned in Section I. In the simulation, each user is assumed to have a tethering device and move around cities based on the check-in data of an actual location-based social network.

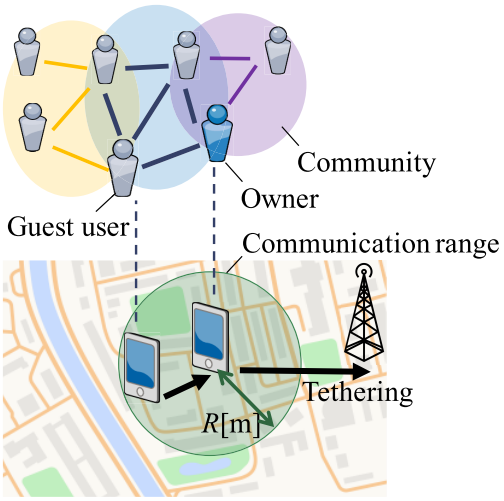

FIGURE 4. Evaluation scenario.

Figure 4 illustrates the evaluation scenario. The simulation takes into account tethering in cellular networks: guest users who are not directly connected to cellular networks send/receive data via a device owner's smartphone. The system in the simulation determines the authorized connection time by evaluating the social closeness defined in Section III-B.2 in an undirected friendship network from an SNS. Requests are sometimes blocked due to the limit of the request queue size or the number of connections to the owner's device.

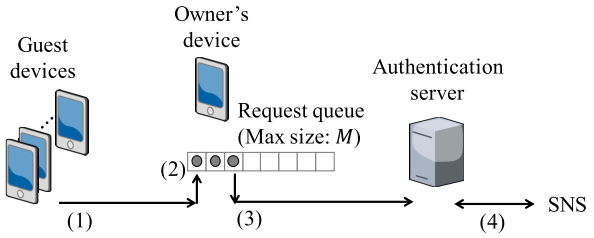

FIGURE 5. Simulation flow.

Figure 5 shows the flow of the simulation. (1) When the owner and a guest user are located within a feasible communication range, the guest user sends a connection request to the owner's device. (2) The owner's device adds the request to a request queue. (3) The owner's device sends a request to the authentication server. (4) The authentication server determines the authorized connection time according to the social closeness between the guest user and owner of the tethering device.

2) EVALUATION MODEL

The parameters of the simulation are listed in Table 4. The detailed explanations of the parameters and components of the simulation are as follows.

TABLE 4. Simulation parameters.

Parameter	Value
Simulation period	Apr. 2008 – Oct. 2010
Radius of communication range (R)	100 m
Max. duration for users to stay at same location (T)	60 minutes
Max. no. of simultaneous connections (N)	5
Authentication latency (L), measured in Sect. IV-A	5.408 seconds
No. of guest users (V)	3,013
Max. size of request queue (M)	10
Mean of requested time in compared system (m)	60 minutes

a: AUTHENTICATION SERVER

The authentication server receives connection requests from the users and determines the authorized connection time for each user. When the authentication server receives a request, it adds the request to the request queue. The size of the request queue is limited to M. If the authentication server receives a request when the request queue is full, the request will be blocked.

The authentication latency is defined as L. In this simulation, the actual measured value mentioned in Section IV-A.3 is used for L.

b: SHARED DEVICE

The tethering devices are shared with users and allow guest devices of authorized users to transmit a certain amount of data through it. The tethering devices can be accessed by up to N guest devices at the same time. Once the number of connected devices reaches N, all subsequent requests will be blocked until the authorized connection time of one of the connected devices expired.

c: OWNER

The relationships with the owner of the WiFi AP determine the authorized connection time for users, and 10% of the users in the dataset are randomly selected as candidates for owners. The simulation was conducted repeatedly for each owner selected from the candidates. The owners are assumed to stay in the i-th check-in location for $\min(T, t_{i+1} - t_i)$ minutes before she or he moves to the next check-in location, where t_i and t_{i+1} are the i-th and $(i+1)$-th check-in times for the owner, respectively.

d: GUEST USERS

The guest users create connection requests and transmit data through the tethering device when authorized. The guest users are assumed to stay in the same location for a certain period as well as the owners.

e: COMMUNICATION RANGE

A communication range is a range within a radius R from the current location of the owner. As the owner and guest users move around, when a guest user enters the communication range of the owner, the guest user makes a connection request to the owner's tethering device. On the other hand, when the owner or guest user leaves the current check-in location and the guest user is no longer within the communication range of the owner, all connection requests and connections to the owner are canceled at that point.

f: AUTHORIZED CONNECTION TIME

The system determines the authorized connection time for each guest user according to the social closeness between the guest user and owner and the communities they belong to. If a guest user U_g is not blocked due to the limit of the request queue size or the number of connections at the owner's tethering device, the authorized connection time for U_g is defined as $\tau(U_g) = SC(U_o, U_g)\beta$, where U_o is the owner, $SC(U_i, U_j)$ is the social closeness between users U_i and U_j, as defined in (6), and β is a coefficient. In this simulation, the common neighbors, Jaccard Index, and Adamic-Adar Index defined in (1) in Section II-C are used as $E(U_o, U_g)$. The value for β is selected so that $\tau(U_g)$ does not exceed T for almost all user pairs.

3) DATASET

In this simulation, Brightkite datasets [44] were used as the data source of online social relationship. Brightkite is a popular online location-based social network. The friendship network of Brightkite was originally directed but was reconstructed as a network with undirected edges by only considering bi-directional edges [45]. To simplify the simulation, users who have at least one check-in in Japan are extracted. Friendships among the extracted users and communities detected by the Link communities algorithm [34] are used to evaluate social relationships between device owners and guest users. The statistics about the extracted users are as follows.

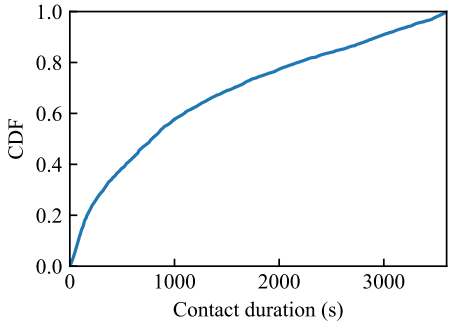

FIGURE 6. Contact duration per contact.

Figure 6 shows the cumulative distribution function (CDF) curve of contact duration per contact. A contact starts when a guest user enters the communication range of the owner and ends when the guest user leaves it. The figure shows that about 50% of contacts were longer than 800 seconds. The maximum contact duration was limited to 3600 seconds because it cannot exceed T. Figure 7 shows the CDF curve

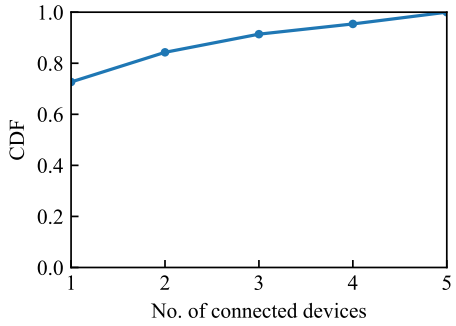

FIGURE 7. No. of connected devices.

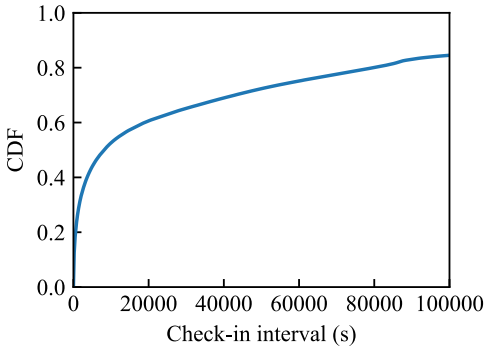

FIGURE 8. Check-in interval.

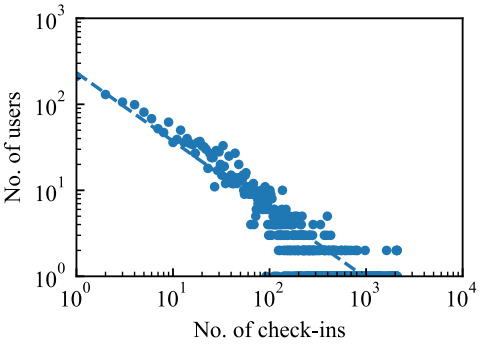

FIGURE 9. No. of users vs. no. of check-ins.

of the number of devices connected to the tethering device over time. The maximum number of connected devices was limited to N. For about 70% of the time, the tethering device was connected by one guest user. Figure 8 shows the CDF curve of intervals of user check-ins. This figure illustrates that about 60% of check-ins were created within 6 hours from a previous check-in. Figure 9 is a double logarithmic chart that shows the number of users against the number of check-ins with a fitted curve having a slope of -0.79. When the number of check-ins was smaller than 100, the number of users decreased along the fitted curve as the number of check-ins increased, whereas when the number of check-ins was greater than 100, the number of users decreased faster than the fitted curve. Figure 10 is a double logarithmic chart that shows the number of user pairs against the number of common neighbors for all $(V-1)V/2$ user pairs with a fitted curve having a slope of -1.94. When the number of common neighbors was smaller than 60, the number of

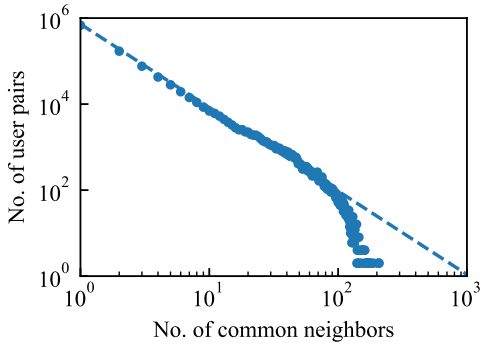

FIGURE 10. No. of user pairs vs. no. of common neighbors.

user pairs decreased along the fitted curve as the number of common neighbors increased, whereas when the number of common neighbors was greater than 60, the number of user pairs decreased faster than the fitted curve.

4) COMPARISON SYSTEM

We compared the proposed system with a system that does not evaluate online social relationships when it authenticates users. The authorized connection time is generated according to exponential distributions whose average is m. The guest user is allowed to access the tethering device for the same duration as the guest user requested until she or he leaves the communication range of the owner, regardless of the social closeness between the owner and guest user. The proposed system was compared with the comparison system based on the average actual connected duration per connection request.

5) RESULTS

The following two points can be observed from the results; i) the proposed system limits the resource usage for guest users who are not as close to the device owners, and ii) the overhead of the authentication process in the system does not interfere with the resource sharing with guest users who are close to the device owners.

Figures 11(a), 11(b) and 11(c) plot the average actual connected duration per connection requests against the number of common neighbors, Jaccard Index, and Adamic-Adar Index, respectively. According to the linear approximate line, as the number of common neighbors increased, the average actual connected duration on the proposed system also increased, while there was no significant change on the comparison system.

In Fig. 11(a), when the number of common neighbors was smaller than 90, the guest users had a shorter actual connected duration on the proposed system than the comparison system. As seen in Fig. 6, about 50% of contacts were longer than 800 seconds. However, according to the linear approximate line, the average actual connected duration of the proposed method was shorter than 800 seconds. This is because the average actual connected duration was properly limited by $\tau(U_g)$. This indicates that the proposed system properly limited the authorized level of resource usage for unfamiliar guest users. On the other hand, when the number

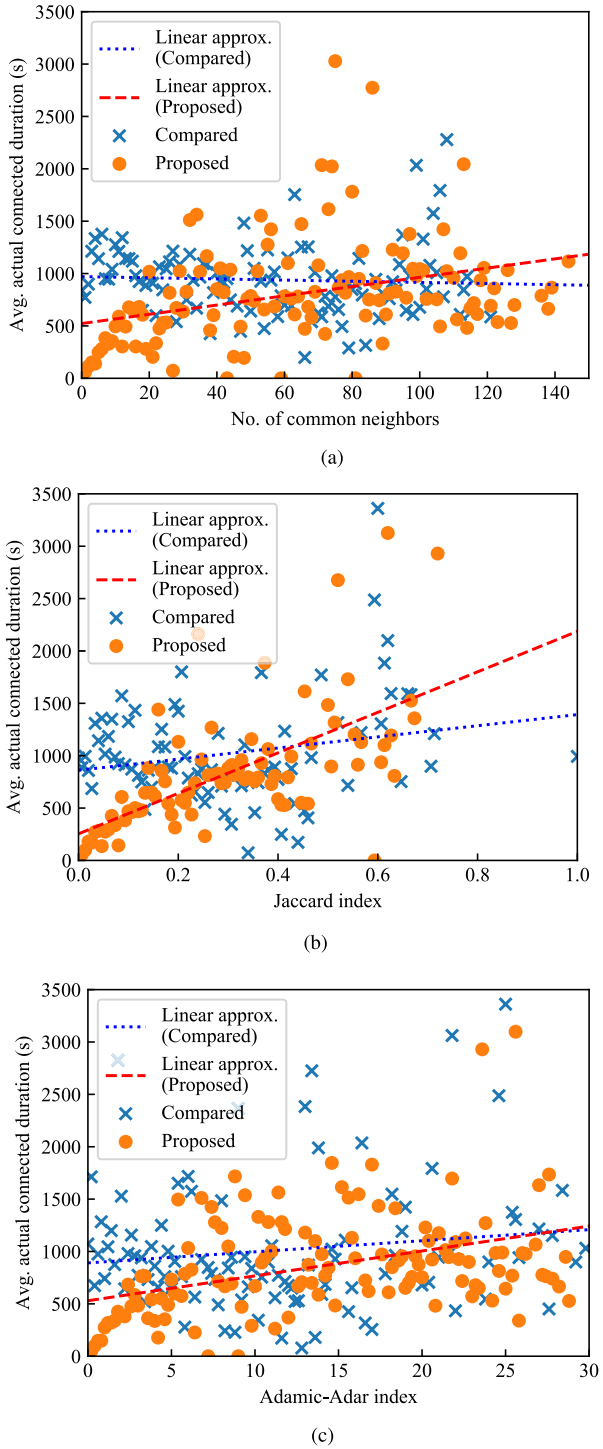

FIGURE 11. Avg. actual connected duration vs. social closeness. (a) common neighbors ($\beta = 1$). (b) Jaccard Index ($\beta = 150$). (c) Adamic-Adar Index ($\beta = 5$).

of common neighbors was greater than 90, the guest users had longer actual connected duration on the proposed system than the comparison system. This is because the authentication latency L, which was set to the actual measured value mentioned in Section IV-A, was much shorter than the average connected duration. Therefore, the proposed system allowed socially close guest users to use the shared devices with only a little interference by its authentication overhead. As a result, points i) and ii) mentioned earlier in this section can be observed from Fig. 11(a).

Figures 11(b) and 11(c) show the same trend as in Fig. 11(a). According to the linear approximate line, when Jaccard Index or Adamic-Adar Index was small, the guest users had a shorter actual connected duration on the proposed system than the comparison system. On the other hand, when Jaccard Index or Adamic-Adar Index was large, the average actual connected duration of the proposed system was longer than that of the comparison system. Therefore, points i) and ii) can also be observed from Figs. 11(b) and 11(c).

V. CONCLUSION

We proposed a system that uses online social relationships to meet device owners' demand for resource management for altruistic device sharing. The proposed system enables device owners to reduce their costs of device sharing with users according to the social closeness between the device owners and guest users. We implemented a prototype system to confirm that the proposed system can be fully implemented as an actual working system and measure the authentication overhead of the proposed system. We also conducted a simulation using this overhead measured on the prototype and a large-scale dataset of a real social network. The simulation verified that i) the proposed system limits the resource usage for guest users who are not as close to the device owners, and ii) the overhead of the authentication process in the system does not interfere with the resource sharing with guest users who are close to the device owners.

As future work, the use of other sources of online social relationships and applications other than tethering will be explored. Future work will also include an incentive mechanism and a privacy issue for both owners and users to use their online social relationships in the proposed system.

VI. ACKNOWLEGMENT

This paper was presented at the 2017 Proceedings of the CQRM Symposium of the IEEE Globecom.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[2] T. Teubner, "Thoughts on the sharing economy," in *Proc. Int. Conf. e-Commerce*, 2014, pp. 322–326.
[3] C. J. Martin, "The sharing economy: A pathway to sustainability or a nightmarish form of neoliberal capitalism?" *Ecol. Econ.*, vol. 121, pp. 149–159, Jan. 2016.
[4] Fon. (2018). *Fon: The Global WiFi Network, Fontech: Leading WiFi Software | Fon*. Accessed: Apr. 7, 2018. [Online]. Available: https://fon.com/
[5] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009.
[6] T. Nishio, R. Shinkuma, T. Takahashi, and N. B. Mandayam, "Service-oriented heterogeneous resource sharing for optimizing service latency in mobile cloud," in *Proc. 1st Int. Workshop Mobile Cloud Comput. Netw.*, 2013, pp. 19–26.
[7] A. Kansal, S. Nath, J. Liu, and F. Zhao, "SenseWeb: An infrastructure for shared sensing," *IEEE MultimediaMag.*, vol. 14, no. 4, pp. 8–13, Oct. 2007.
[8] J. Beal, K. Usbeck, J. Loyall, and J. Metzler, "Opportunistic sharing of airborne sensors," in *Proc. Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2016, pp. 25–32.

[9] J. Beal, K. Usbeck, J. Loyall, M. Rowe, and J. Metzler, "Adaptive task reallocation for airborne sensor sharing," in *Proc. IEEE 1st Int. Workshops Found. Appl. Self Syst. (FAS W)*, Sep. 2016, pp. 168–173.
[10] T. Zhu, Y. Gu, T. He, and Z.-L. Zhang, "eShare: A capacitor-driven energy storage and sharing network for long-term operation," in *Proc. 8th ACM Conf. Embedded Netw. Sensor Syst.*, 2010, pp. 239–252.
[11] N. Eagle and A. Pentland, "Reality mining: Sensing complex social systems," *Pers. Ubiquitous Comput.*, vol. 10, no. 4, pp. 255–268, 2005.
[12] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE rap: Social-based forwarding in delay-tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 11, pp. 1576–1589, Nov. 2011. [Online]. Available: http://ieeexplore.ieee.org/document/5677535/
[13] H. Rachlin and B. A. Jones, "Altruism among relatives and non-relatives," *Behavioural Processes*, vol. 79, no. 2, pp. 120–123, 2008.
[14] O. Curry, S. G. B. Roberts, and R. I. M. Dunbar, "Altruism in social networks: Evidence for a 'kinship premium,'" *Brit. J. Psychol.*, vol. 104, no. 2, pp. 283–295, 2013.
[15] O. Curry and R. I. M. Dunbar, "Altruism in networks: The effect of connections," *Biol. lett.*, vol. 7, no. 5, pp. 651–653, Oct. 2011.
[16] P. Brañas-Garza, R. Cobo-Reyes, M. P. Espinosa, N. Jiménez, J. Kovářík, and G. Ponti, "Altruism and social integration," *Games Econ. Behavior*, vol. 69, no. 2, pp. 249–257, 2010.
[17] F. Harrison, J. Sciberras, and R. James, "Strength of social tie predicts cooperative investment in a human social network," *PLoS ONE*, vol. 6, no. 3, p. e18338, 2011.
[18] M. Yamada, R. Shinkuma, and T. Takahashi, "Cooperative networking in heterogeneous infrastructure multihop mobile networks," in *Proc. IEEE 17th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2006, pp. 1–5.
[19] D. Zhang, R. Shinkuma, and N. B. Mandayam, "Bandwidth exchange: An energy conserving incentive mechanism for cooperation," *IEEE Trans. Wireless Commun.*, vol. 9, no. 6, pp. 2055–2065, Jun. 2010.
[20] P. Shankar, B. Nath, L. Iftode, V. Ananthanarayanan, and L. Han, "SBone: Personal device sharing using social networks," Rutgers Univ., Brunswick, NJ, USA, Tech. Rep. DCS-TR-666, 2010.
[21] X. Wang, M. Chen, T. Kwon, L. Jin, and V. Leung, "Mobile traffic offloading by exploiting social network services and leveraging opportunistic device-to-device sharing," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 28–36, Mar. 2014.
[22] X. Wang and V. C. Leung, "SNS-based mobile traffic offloading by opportunistic device-to-device sharing," in *The Future of Wireless Networks: Architectures, Protocols, and Services*, vol. 21. Boca Raton, FL, USA: CRC Press, 2015, p. 327.
[23] X. Wang, Z. Sheng, S. Yang, and V. C. M. Leung, "Tag-assisted social-aware opportunistic device-to-device sharing for traffic offloading in mobile social networks," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 60–67, Aug. 2016.
[24] C. H. Su, Y.-C. Hwang, and C. C. Yeh, "A study on the willingness of using FON in the domain of wireless communication," in *Proc. 4th Int. Conf. Netw. Comput. Adv. Inf. Manage. (NCM)*, Sep. 2008, pp. 159–164.
[25] T. Hirofuchi, E. Kawai, K. Fujikawa, and H. Sunahara, "USB/IP—A peripheral bus extension for device sharing over IP network," in *Proc. Annu. Conf. USENIX Annu. Tech. Conf.*, 2005, p. 42.
[26] W. Kwon, H. W. Cho, and Y. H. Song, "Design and implementation of peripheral sharing mechanism on pervasive computing with heterogeneous environment," in *Proc. IFIP Int. Workshop Softw. Technol. Embedded Ubiquitous Syst.*, 2007, pp. 537–546.
[27] J. Kong, I. Ganev, K. Schwan, and P. Widener, "CameraCast: Flexible access to remote video sensors," *Proc. SPIE*, vol. 6504, pp. 65040P, Jan. 2007. [Online]. Available: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/6504/1/CameraCast-flexible-access-to-remote-video-sensors/10.1117/12.703490.short
[28] X. Wu, W. Wang, B. Lin, and K. Miao, "Composable IO: A novel resource sharing platform in personal clouds," in *Proc. IEEE Int. Conf. Cloud Comput.*, 2009, pp. 232–242.
[29] N. P. Nguyen, T. N. Dinh, Y. Xuan, and M. T. Thai, "Adaptive algorithms for detecting community structure in dynamic social networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2282–2290.
[30] K. Chard, S. Caton, O. Rana, and K. Bubendorfer, "Social cloud: Cloud computing in social networks," in *Proc. IEEE 3rd Int. Conf. Cloud Comput.*, Jul. 2010, pp. 99–106.
[31] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *IEEE Trans. Services Comput.*, vol. 5, no. 4, pp. 551–563, Jun. 2012.
[32] R. Shinkuma, Y. Sawada, Y. Omori, K. Yamaguchi, H. Kasai, and T. Takahashi, *A Socialized System for Enabling the Extraction of Potential Values From Natural and Social Sensing*. Cham, Switzerland: Springer, 2015, pp. 385–404. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-09177-8_16
[33] M. Nakahara, R. Shinkuma, K. Yamaguchi, and K. Yamaguchi, "Tradeoff between privacy protection and network resource in community associated network virtualization," in *Proc. IEEE 26th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Aug./Sep. 2015, pp. 2143–2148.
[34] Y.-Y. Ahn, J. P. Bagrow, and S. Lehmann, "Link communities reveal multiscale complexity in networks," *Nature*, vol. 466, no. 7307, pp. 761–764, 2010.
[35] L. Lü and T. Zhou, "Link prediction in complex networks: A survey," *Phys. A, Statist. Mech. Appl.*, vol. 390, no. 6, pp. 1150–1170, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S037843711000991X
[36] P. Jaccard, "The distribution of the flora in the alpine zone. 1," *New Phytol.*, vol. 11, no. 2, pp. 37–50, 1912. [Online]. Available: http://dx.doi.org/10.1111/j.1469-8137.1912.tb05611.x
[37] L. A. Adamic and E. Adar, "Friends and neighbors on the Web," *Soc. Netw.*, vol. 25, no. 3, pp. 211–230, 2003.
[38] L. Katz, "A new status index derived from sociometric analysis," *Psychometrika*, vol. 18, no. 1, pp. 39–43, 1953. [Online]. Available: https://doi.org/10.1007/BF02289026
[39] L. Garton, C. Haythornthwaite, and B. Wellman, "Studying online social networks," *J. Comput.-Mediated Commun.*, vol. 3, no. 1, 1997.
[40] Bumbeelabs.com. (2018). *Bumbee Labs—WIFI-Based Visitor Flows*. Accessed: Apr. 7, 2018. [Online]. Available: https://www.bumbeelabs.com/en
[41] T. Kaya and H. Bicen, "The effects of social media on students' behaviors; Facebook as a case study," *Comput. Hum. Behavior*, vol. 59, pp. 374–379, Jun. 2016.
[42] D. Hardt, *RFC 6749—The OAuth 2. 0 Authorization Framework*. Fremont, CA, USA: Internet Engineering Task Force, 2012.
[43] H. Annuar, B. Shanmugam, A. Ahmad, N. B. Idris, S. H. AlBakri, and G. N. Samy, "Enhancement and implementation of network access control architecture for virtualization environments," in *Proc. Int. Conf. Informat. Creative Multimedia*, Sep. 2013, pp. 314–320.
[44] Snap.stanford.edu. (2018). *SNAP: Network Datasets: Brightkite*. Accessed: Apr. 7, 2018. [Online]. Available: https://snap.stanford.edu/data/loc-brightkite.html
[45] E. Cho, S. A. Myers, and J. Leskovec, "Friendship and mobility: User movement in location-based social networks," in *Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2011, pp. 1082–1090.

YUICHI INAGAKI received the B.E. degree in electrical and electronic engineering from Kyoto University, Kyoto, Japan, in 2017, where he is currently pursuing the degree in communications and computer engineering with the Graduate School of Informatics. His research interests include system design in IoT applications.

RYOICHI SHINKUMA received the B.E., M.E., and Ph.D. degrees in communications engineering from Osaka University, Osaka, Japan, in 2000, 2001, and 2003, respectively. In 2003, he joined the Communications and Computer Engineering, Graduate School of Informatics, Kyoto University, as an Associate Professor. He was a Visiting Scholar with the Wireless Information Network Laboratory, Rutgers, The State University of New Jersey, USA, from 2008 to 2009. His research interests include network design and control criteria, particularly inspired by economic and social aspects. He is a Senior Member of IEICE. He received the Young Researchers' Award from IEICE in 2006, the Young Scientist Award from Ericsson Japan in 2007, and the TELECOM System Award from the Telecommunications Advancement Foundation in 2016. He has been the Chairperson with the Mobile Network and Applications Technical Committee of the IEICE Communications Society since 2017.